Claims

1. An information processing system for distributing encrypted message data capable of being used only in not less than one device selected,

said individual device comprising:

encryption processing means for holding a different key set of a node key peculiar to each node in a hierarchical tree structure having a plurality of different devices as leaves and a leaf key peculiar to each device and executing decrypting process of said encrypted message data distributed to a device using said key set;

wherein the encrypted message data distributed to said device has data constitution to be encrypted with a renewal node key obtained in a decrypting process of an enabling key block (EKB) including encrypted key data into which the renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure is encrypted by the node key or the leaf key in said group, and

said enabling key block (EKB) includes a data part constituted by said encrypted key data and a tag part as position discrimination data of the encrypted key data in said hierarchical tree structure.

2. The information processing system according to claim 1 wherein said encrypted key data included in said enabling key block (EKB) is data into which a node key constituting said hierarchical tree structure is encrypted using a

subordinate node key or a subordinate leaf key, and

position discrimination data stored in said tag part is constituted as a tag indicating whether there is the encrypted key data at subordinate left and right node or leaf position of a node position of each of not less than one encrypted key data stored in said enabling key block (EKB) or not.

3. The information processing system according to claim 1 wherein said encrypted key data included in said enabling key block (EKB) is constituted on the basis of only keys corresponding to a node or a leaf of a reconstructed hierarchical tree reconstructed by selecting paths constituting a simplified 2-branched type tree with terminal nodes or leaves with which the enabling key block (EKB) can be decrypted at the lowest stage to omit unnecessary nodes, and

position discrimination data stored in said tag part includes data indicating whether the encrypted key corresponding to the tag of said enabling key block (EKB) is stored or not.

4. The information processing system according to claim 1 wherein said encrypted key data included in said enabling key block (EKB) is constituted on the basis of only a key corresponding to a node or a leaf of a reconstructed hierarchical tree reconstructed by selecting paths constituting a simplified 2-branched type tree with terminal nodes or leaves with which the enabling key block (EKB) can be decrypted at the lowest stage to omit unnecessary nodes, and position discrimination data stored in said tag part includes tags indicating whether

encrypted key data at left and right node or leaf position at subordinate of a node position of each of not less than one encrypted key data stored in said enabling key block (EKB), and data indicating whether the encrypted key corresponding to said tag is stored or not.

5. The information processing system according to claim 4 wherein said reconstructed hierarchical tree is a tree constituted by selecting a sub-root which is a top node of an entity defined as a subset tree of devices having a common element.

6. The information processing system according to claim 1 wherein said encrypted key data included in said enabling key block (EKB) is constituted, in a simplified multi-branched type tree having terminal node or leaf with which the enabling key block (EKB) can be decrypted at the lowermost stage, on the basis of only keys corresponding to a top node and terminal nodes or leaves of a reconstructed hierarchical tree reconstructed by selecting paths directly connecting said terminal nodes or leaves and a top of the multi-branched type tree to omit an unnecessary node, and

position discrimination data stored in said tag part includes data indicating whether an encrypted key corresponding to the tag of said enabling key block (EKB) is stored or not.

7. The information processing system according to claim 6 wherein said reconstructed hierarchical tree is a tree having not less than three branches

connecting the top node constituting the simplified multi-branched type tree with terminal nodes or leaves constituting the simplified tree directly.

8. The information processing system according to claim 1 wherein said encryption processing means in said device has a constitution for sequentially extracting said encrypted key data with data of said tag part in said enabling key block (EKB), executing decrypting process to obtain the renewal node key, and executing decryption of said encrypted message data with the renewal node key obtained.

9. The information processing system according to claim 1 wherein said message data is a content key that can be used as a decryption key for decrypting content data.

10. The information processing system according to claim 1 wherein said message data is an authentication key used in the authentication process.

11. The information processing system according to claim 1 wherein said message data is a key for generating an integrity check value (ICV) of the content.

12. The information processing system according to claim 1 wherein said message data is a program code.

13. An information processing method for distributing encrypted message data capable of being used only in not less than one selected devices, comprising:

an enabling key block (EKB) generating step of generating an enabling key block (EKB) including a data part including encrypted key data into which the

renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected at subordinate of a top node which is one node of the hierarchical tree structure is renewed is encrypted with a node key or a leaf key in said group, and a tag part which is position discrimination data in the hierarchical tree structure of encrypted key data stored in the data part; and

a message data distribution step for generating message data encrypted with said renewal node key to distribute it to a device.

14. The information processing method according to claim 13, further comprising a decrypting processing step of executing decrypting process to said encrypted message data using the key set in a device holding a different key set of a node key peculiar to each node in the hierarchical structure and a leaf key peculiar to each device.

15. The information processing method according to claim 13 wherein said enabling key block (EKB) generating step includes a step of encrypting a node key constituting said hierarchical tree structure using a subordinate node key or a subordinate leaf key to generate said encrypted key data, and

a step of generating a tag indicating whether there is encrypted key data at a node or leaf position at subordinate left and right positions of a node position of each of not less than one encrypted key data stored in said enabling key block (EKB) or not to store it in said tag part.

16. The information processing method according to claim 13 wherein said

enabling key block (EKB) generating step includes a step of generating a reconstructed hierarchical tree by selecting paths constituting a simplified 2-branched type tree with a terminal node or leaf capable of decrypting the enabling key block (EKB) at the lowest stage to omit unnecessary nodes;

a step of generating an enabling key bock (EKB) on the basis of only a key corresponding to a constitution node or leaf of said reconstructed hierarchical tree; and

a step of storing data indicating whether an encrypted key corresponding to a tag of said enabling key block (EKB) is stored in said tag part or not.

17. The information processing method according to claim 16 wherein said step of generating the reconstructed hierarchical tree is tree generating processing executed by selecting a sub-root which is a top node of entity defined as a subset tree of devices having a common element.

18. The information processing method according to claim 13 wherein said enabling key block (EKB) generating step includes a step of generating, in the simplified branched type tree with a terminal node or leaf capable of decrypting the enabling key bock (EKB) at the lowest stage, the reconstructed hierarchical tree reconstructed by selecting a path for directly connecting the terminal node or leaf with the top of the multi-branched type tree; and

a step of storing data indicating whether an encrypted key corresponding to a tag of said enabling key bock (EKB) is stored in the tag part or not.

19. The information processing method according to claim 18 wherein said reconstructed hierarchical tree generated in the step of generating the reconstructed hierarchical tree is generated as a tree having not less than three branches having a top node constituting a simplified multi-branched type tree and a terminal node or leaf constituting a simplified tree connected directly.

20. The information processing method according to claim 14 wherein said decrypting processing step includes a renewal node key obtaining step of obtaining said renewal node key by sequentially extracting encrypted key data stored in the data part on the basis of position discrimination data stored in the tag part of the enabling key block (EKB) to sequentially execute decrypting process; and

a message data decrypting step for executing decryption of the encrypted message data with said renewal node key.

21. The information processing method according to claim 13 wherein said message data is a content key capable of being used as a decryption key for decrypting the content data.

22. The information processing method according to claim 13 wherein said message data is an authentication key used in the authentication process.

23. The information processing method according to claim 13 wherein said message data is a key of generating an integrity check value (ICV) of contents.

24. The information processing method according to claim 13 wherein said message data is a program code.

25. An information recording medium having data stored, storing:

an enabling key block (EKB) including a data part including encrypted key data into which the renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected under a top node which is one node of the hierarchical tree structure is renewed is encrypted with a node key or a leaf key in said group, and a tag part which is position discrimination data in the hierarchical tree structure of encrypted key data stored in the data part, and

message data encrypted by said renewal node key.

26. The information recording medium according to claim 25 where said encrypted key data included in the enabling key block (EKB) is data into which the node key constituting the hierarchical tree structure is encrypted using a subordinate node key or a subordinate leaf key; and

said position discrimination data stored in the tag part is constituted as a tag indicating whether there is key data at the node of leaf position at the subordinate left and right positions of the node position of each of not less one encrypted key data stored in the enabling key block (EKB).

27. The information recording medium according to claim 25 wherein said encrypted key data included in said enabling key block (EKB) is constituted on the basis of only a key corresponding to a node or a leaf of a reconstructed hierarchical tree reconstructed by selecting paths constituting a simplified 2-branched type tree with a terminal node or leaf capable of decrypting the enabling key block (EKB) at

the lowest stage to omit unnecessary nodes; and

said position discrimination data stored in said tag part includes data indicating whether an encrypted key corresponding to the tag of the enabling key block (EKB) is stored or not.

28. A program distributing medium for distributing a computer program to execute on a computer system a process of generating an enabling key block (EKB) into which a renewal node key into which at least one of the node keys in a group constituted by nodes and a leaves connected under said top node which is one node of the hierarchical tree structure is renewed is encrypted with a node key or a leaf key in said group,

said computer program including:

a step of generating a reconstructed hierarchical tree by selecting a path constituting a simplified 2-branched type tree with a terminal node or a leaf capable of decrypting the enabling key block (EKB) at the lowest stage to omit an unnecessary node;

a step of generating the enabling key block (EKB) on the basis of only a key corresponding to a constitution node or leaf of said reconstructed hierarchical tree; and

a step of storing data indicating whether an encrypted key corresponding to a tag of said enabling key block (EKB) is stored or not.

29. An information processing apparatus comprising:

storage means for holding a key set of a peculiar node key and a leaf key in a hierarchical tree structure with a plurality of different devices as a leaf; and

decrypting processing means for executing decrypting process to encrypted message data distributed, using said key set;

wherein the encrypted message data distributed has data constitution to be encrypted with a renewal node key obtained in a decrypting process of an enabling key block (EKB) of said decrypting processing means , and

wherein said enabling key bock (EKB) includes:

a data part constituted by encrypted key data into which said renewal node key into which at least any one of the node keys in a group constituted by nodes and leaves connected under a top node which is one node of the hierarchical tree structure is encrypted with a node key or a leaf key in said group; and

a tag part as position discrimination data in said hierarchical tree structure of the encrypted key data stored in said data part.

30. The information processing apparatus according to claim 29 wherein said encrypted key data included in said enabling key block (EKB) is data into which a node key constituting said hierarchical tree structure is encrypted using a subordinate node key or a subordinate leaf key, and

position discrimination data stored in said tag part is constituted as a tag indicating whether the key data at the node of leaf position at the subordinate left and right positions of the node position of each of not less one encrypted key data

stored in the enabling key block (EKB).

31. The information processing apparatus according to claim 29 wherein said encrypted key data included in said enabling key block (EKB) is constituted on the basis of only a key corresponding to a node or a leaf of a reconstructed hierarchical tree reconstructed by selecting paths constituting a simplified branched type tree with a terminal node or leaf capable of decrypting the enabling key block (EKB) at the lowest stage to omit unnecessary nodes, and

position discrimination data stored in said tag part includes data indicating whether an encrypted key corresponding to the tag of said enabling key block (EKB) is stored or not.

32. The information processing apparatus according to claim 29 wherein said encrypted key data included in said enabling key block (EKB) is constituted on the basis of only a key corresponding to a node or a leaf of a reconstructed hierarchical tree reconstructed by selecting paths constituting a simplified branched type tree with a terminal node or leaf capable of decrypting the enabling key block (EKB) at the lowest stage to omit unnecessary nodes, and

position discrimination date stored in said tag part is a constitution including a tag indicating whether the key data at the node of leaf position at the subordinate left and right positions of the node position of each of not less one encrypted key data stored in the enabling key block (EKB), and data indicating whether an encrypted key corresponding to said tag is stored or not.

33. The information processing apparatus according to claim 29 wherein said decrypting processing means has a constitution for sequentially extracting said encrypted key data with data of said tag part in said enabling key block (EKB), executing decrypting process to obtain the renewal node key, and executing decryption of said encrypted message data with the renewal node key obtained.

34. An information processing method for executing decrypting process on encrypted message data distributed, said method comprising:

an encrypted key data obtaining step of obtaining encrypted key data from an enabling key block (EKB) including said encrypted key data into which a renewal node key into which at least one of the node keys in a group constituted by nodes and leaves connected under a top node which is one node of the hierarchical tree structure is renewed is encrypted with a node key or a leaf key in said group; and

a renewal node key obtaining step of obtaining said renewal node key by decrypting said encrypted key data obtained,

wherein said enabling key bock (EKB) includes a data part constituted by said encrypted key data and a tag part as position discrimination data in said hierarchical tree structure of the encrypted key data.

35. The information processing method according to claim 34 wherein in said encrypted key data obtaining step, encrypted key data stored in the data part is sequentially extracted on the basis of position discrimination data stored in the tag part of the enabling key block (EKB),

wherein in said renewal node key obtaining step, decrypting process is sequentially executed on said encrypted key data obtained to obtain said renewal node key; and further comprising:

a decrypting processing step of executing decryption of the encrypted message data by said renewal node key.

36. The information processing method according to claim 35, wherein in said decrypting processing step, a different key set of a node key peculiar to each node and a leaf key peculiar to each device in the hierarchical structure is held, and decrypting process is executed with respect to said encrypted message data using the key set.

37. The information processing method according to claim 34 wherein said message data is a content key capable of being used as a decryption key for decrypting the content data.

38. The information processing method according to claim 34 wherein said message data is an authentication key used in the authentication processing.

39. The information processing method according to claim 34 wherein said message data is a key of generating an integrity check value (ICV) of contents.